EIROPAS KOMISIJA

EIROPAS SAVIENĪBAS AUGSTĀ PĀRSTĀVE ĀRLIETĀS UN DROŠĪBAS POLITIKAS JAUTĀJUMOS

Briselē, 7.2.2013
JOIN(2013) 1 final

KOPĪGS PAZIŅOJUMS EIROPAS PARLAMENTAM, PADOMEI, EIROPAS EKONOMIKAS UN SOCIĀLO LIETU KOMITEJAI UN REĢIONU KOMITEJAI

Eiropas Savienības kiberdrošības stratēģija –

atvērta un droša kibertelpa

KOPĪGS PAZIŅOJUMS EIROPAS PARLAMENTAM, PADOMEI, EIROPAS EKONOMIKAS UN SOCIĀLO LIETU KOMITEJAI UN REĢIONU KOMITEJAI

Eiropas Savienības kiberdrošības stratēģija –

atvērta un droša kibertelpa

1. IEVADS

1.1. Konteksts

Pēdējo divdesmit gadu laikā internetam un kibertelpai kopumā ir bijusi milzīga ietekme uz visām sabiedrības grupām. Mūsu ikdienas dzīve, pamattiesības, sociālā mijiedarbība un tautsaimniecība ir atkarīga no informācijas un komunikācijas tehnoloģiju netraucētas darbības. Atvērta un brīva kibertelpa ir veicinājusi politisku un sociālu iekļaušanu pasaules mērogā; tā ir palīdzējusi novērst šķēršļus starp valstīm, cilvēku grupām un iedzīvotājiem, ļaujot mijiedarboties un apmainīties ar informāciju un idejām visā pasaulē; tā ir nodrošinājusi forumu vārda brīvībai un pamattiesību īstenošanai un palīdzējusi cilvēkiem veidot demokrātiskas un taisnīgākas sabiedrības – uzskatāmākais piemērs ir Arābu pavasaris.

Lai kibertelpa varētu palikt atvērta un brīva, tās pašas normas, principi un vērtības, ko ES atbalsta bezsaistē, būtu jāpiemēro arī tiešsaistē. Kibertelpā ir jāaizsargā pamattiesības, demokrātija un tiesiskums. Mūsu brīvība un labklājība arvien vairāk ir atkarīga no stabila un novatoriska interneta, kurš turpinās attīstīties, ja tā izaugsmi veicinās privātā sektora inovācija un pilsoniskā sabiedrība. Taču brīvībai tiešsaistē nepieciešama arī drošība un drošums. Kibertelpa jāaizsargā no incidentiem, ļaunprātīgām darbībām un ļaunprātīgas izmantošanas, un valdībām ir būtiska loma brīvas un drošas kibertelpas nodrošināšanā. Valdībām ir vairāki uzdevumi: nodrošināt piekļuvi un atvērtību, ievērot un aizsargāt pamattiesības tiešsaistē, nodrošināt interneta uzticamību un sadarbspēju. Tomēr būtiska kibertelpas daļa pieder privātajam sektoram, un privātais sektors nodrošina tās darbību, tāpēc jebkurā iniciatīvā, kuras mērķis ir gūt sekmes šajā jomā, ir jāņem vērā šī sektora vadošā loma.

Informācijas un komunikācijas tehnoloģijas ir kļuvušas par mūsu ekonomiskās izaugsmes pamatu, un tās ir svarīgs resurss, kuru izmanto visās tautsaimniecības nozarēs. Pašlaik tās ir pamatā kompleksām sistēmām, kuras uztur tautsaimniecības darbību tādās būtiskās nozarēs kā finanses, veselības aprūpe, enerģētika un transports, un daudzi uzņēmējdarbības modeļi balstās uz nepārtrauktu interneta pieejamību un informācijas sistēmu netraucētu darbību.

Pabeidzot digitālā vienotā tirgus izveidi, Eiropa varētu palielināt IKP par aptuveni 500 miljardiem euro gadā[1], kas atbilst 1000 euro uz cilvēku. Lai varētu izplatīties jaunās savienotās tehnoloģijas, tostarp e-maksājumi, mākoņdatošana vai iekārtu komunikācijas sistēmas[2], ir nepieciešama iedzīvotāju uzticēšanās un paļāvība. Diemžēl 2012. gada Eirobarometra aptauja[3] liecina, ka gandrīz trešdaļa eiropiešu nav pārliecināti par savām spējām izmantot internetu bankas pakalpojumiem tiešsaistē vai pirkumiem. Lielākā daļa aptaujāto arī teica, ka viņi izvairās no personiskas informācijas izpaušanas tiešsaistē drošības apsvērumu dēļ. Eiropas Savienībā vairāk nekā katrs desmitais interneta lietotājs jau ir kļuvis par tiešsaistes krāpšanas upuri.

---

1 http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf.

2 Piemēram, augos ievietoti sensori, kas paziņo smidzinātājsistēmai, kad augi ir jāaplaista.

3 2012. gada īpašā Eirobarometra aptauja Nr. 390 par kiberdrošību.

Pēdējos gados ir atklājies: lai gan digitālā pasaule sniedz milzīgus ieguvumus, tā ir arī neaizsargāta. Kiberdrošības[4] incidentu – tīšu vai nejaušu – skaits palielinās satraucošā ātrumā un varētu traucēt tādu būtisku pakalpojumu sniegšanai, kurus mēs uzskatām par pašsaprotamiem, piemēram, ūdens apgāde, veselības aprūpe, elektroenerģijas piegāde vai mobilo sakaru pakalpojumi. Draudiem var būt dažāda izcelsme – tostarp krimināli, politiski motivēti, terora akti vai valsts atbalstīti uzbrukumi, kā arī dabas katastrofas vai netīšas kļūdas.

ES ekonomiku jau ietekmē kibernoziedzības[5] darbības, kas vērstas pret privāto sektoru un indivīdiem. Kibernoziedznieki izmanto arvien izsmalcinātākas metodes, lai ielauztos informācijas sistēmās, nozagtu svarīgus datus vai no uzņēmumiem pieprasītu izpirkšanas maksu. Ekonomiskās spiegošanas pieaugums un valsts atbalstīta darbība kibertelpā veido jaunu draudu kategoriju ES dalībvalstu valdībām un uzņēmumiem.

Valstīs ārpus ES valdības var arī ļaunprātīgi izmantot kibertelpu, lai uzraudzītu un kontrolētu savus iedzīvotājus. ES var vērsties pret šo situāciju, veicinot brīvību un nodrošinot pamattiesību ievērošanu tiešsaistē.

Visi šie faktori izskaidro, kāpēc valdības visā pasaulē ir sākušas izstrādāt kiberdrošības stratēģijas un uzskatīt kibertelpu par arvien svarīgāku valsts jautājumu. Ir pienācis laiks ES darboties aktīvāk šajā jomā. Komisijas un Savienības Augstās pārstāves ārlietās un drošības politikas jautājumos (Augstā pārstāve) ierosinātajā priekšlikumā par Eiropas savienības kiberdrošības stratēģiju ir izklāstīts ES skatījums uz šo jomu, precizētas funkcijas un pienākumi un noteiktas nepieciešamās darbības, kuru pamatā ir pilsoņu tiesību spēcīga un efektīva aizsardzība un piemērošana, lai padarītu ES tiešsaistes vidi par drošāko pasaulē.

1.2. Kiberdrošības principi

Bezrobežu un daudzlīmeņu internets ir kļuvis par vienu no spēcīgākajiem instrumentiem globālajā virzībā uz priekšu bez valdības pārraudzības vai regulējuma. Privātajam sektoram būtu jāturpina uzņemties vadošā loma interneta izveidē un pārvaldību ikdienā, tomēr arvien izteiktāka kļūst vajadzība pēc pārredzamības, atbildības un drošības prasībām. Šajā stratēģijā ir precizēti principi, kuriem vajadzētu būt kiberdrošības politikas pamatā ES un starptautiskā mērogā.

ES pamatvērtības vienādā mērā attiecas gan uz digitālo, gan reālo pasauli

Tie paši likumi un normas, kas tiek piemērotas mūsu ikdienas dzīves citās jomās, attiecas arī uz kibersfēru.

Pamattiesību, vārda brīvības, personas datu un privātuma aizsardzība

Kiberdrošība var būt saprātīga tikai tad, ja tā balstās uz pamattiesībām un brīvībām, kā paredzēts Eiropas Savienības Pamattiesību hartā un ES pamatvērtībās. Tieši tāpat indivīda

---

[4] Kiberdrošība parasti nozīmē drošības pasākumus un darbības, ko var izmantot, lai aizsargātu kibersfēru gan civilās, gan militārās jomās no tādiem draudiem, kas ir saistīti ar tās savstarpēji atkarīgiem tīkliem un informācijas infrastruktūru vai var tām kaitēt. Kiberdrošības mērķis ir aizsargāt tīklu un infrastruktūru pieejamību un intergitāti, kā arī tajos ietvertās informācijas konfidencialitāti.

[5] Kibernoziedzība parasti nozīmē dažādu noziedzīgu darbību plašu spektru, kuras ir saistītas ar datoriem un informācijas sistēmām kā galveno līdzekli vai galveno mērķi. Kibernoziedzība ietver tradicionālus pārkāpumus (piemēram, krāpšana, viltošana, identitātes zādzība), ar saturu saistītus pārkāpumus (piemēram, bērnu pornogrāfijas izplatīšana tiešsaistē vai kūdīšana uz rasu naidu) un pārkāpumus, kas saistīti vienīgi ar datoriem un informācijas sistēmām (piemēram, uzbrukumi informācijas sistēmām, pakalpojumatteice un ļaunprātīga programmatūra).

tiesības nevar nodrošināt, ja nav drošu tīklu un sistēmu. Jebkurai informācijas apmaiņai kiberdrošības nolūkā, ja ir iesaistīti personas dati, ir jābūt saskaņā ar ES datu aizsardzības tiesību aktiem un pilnībā jāņem vērā indivīda tiesības šajā jomā.

Vispārēja piekļuve

Ierobežota piekļuve internetam vai tās trūkums un digitālā nekompetence nostāda iedzīvotājus neizdevīgā stāvoklī, ņemot vērā to, cik ļoti digitālā pasaule ir saistīta ar darbību sabiedrībā. Visiem būtu jābūt iespējai piekļūt internetam un netraucētai informācijas plūsmai. Ir jāgarantē interneta integritāte un drošība, lai nodrošinātu drošu vispārēju piekļuvi.

Demokrātiska un efektīva daudzu ieinteresētu personu īstenota pārvaldība

Digitālo pasauli nekontrolē viena struktūra. Pašlaik ir vairākas ieinteresētās personas (no kurām liela daļa ir komercuzņēmumi un nevalstiskas struktūras), kas ir iesaistījušās interneta resursu, protokolu un standartu ikdienas pārvaldībā un interneta turpmākajā attīstībā. ES vēlreiz apstiprina, cik svarīgas ir visas ieinteresētās personas pašreizējā interneta pārvaldības modelī, un atbalsta daudzu ieinteresētu personu īstenotas pārvaldības pieeju[6].

Kopīga atbildība par drošību

Arvien lielāka atkarība no informācijas un komunikācijas tehnoloģijām visās cilvēka dzīves jomās ir radījusi neaizsargātību, kuru nepieciešams atbilstīgi definēt, rūpīgi analizēt, novērst vai samazināt. Visiem attiecīgiem dalībniekiem – publiskām iestādēm, privātajam sektoram vai atsevišķiem iedzīvotājiem – jāatzīst šī kopīgā atbildība, jārīkojas, lai sevi aizsargātu, un, ja nepieciešams, jānodrošina saskaņota reaģēšana kiberdrošības stiprināšanai.

2. STRATĒĢISKĀS PRIORITĀTES UN DARBĪBAS

ES jānodrošina visiem iedzīvotājiem tiešsaistes vide, kurā ir augstākais iespējamais brīvības un drošības līmenis. Atzīstot, ka drošības problēmu risināšana kibertelpā ir galvenokārt dalībvalstu uzdevums, šajā stratēģijā ierosinātas konkrētas darbības, kas var uzlabot ES vispārējo sniegumu. Ir paredzētas gan īstermiņa, gan ilgtermiņa darbības, kuras ietver dažādus politikas instrumentus[7] un kurās iesaistīti dažādi dalībnieku veidi: ES iestādes, dalībvalstis vai nozares pārstāvji.

Šajā stratēģijā izklāstītais ES redzējums ir sadalīts piecās prioritātēs, kas attiecas uz iepriekš aprakstītajām problēmām:

- kibernoturības panākšana;
- kibernoziedzības būtiska samazināšana;
- kiberaizsardzības politikas izstrāde un spēju veidošana saistībā ar kopējo drošības un aizsardzības politiku (KDAP);
- rūpniecisko un tehnoloģisko resursu veidošana kiberdrošības vajadzībām;
- saskaņotas starptautiskas kibertelpas politikas izveide Eiropas Savienībā un ES pamatvērtību popularizēšana.

---

[6] Sk. arī COM(2009) 277, Komisijas paziņojums Eiropas Parlamentam un Padomei „Interneta pārvaldība – turpmāk veicamie pasākumi".

[7] Darbībām, kas saistītas ar informācijas apmaiņu, kurā iesaistīti personas dati, ir jābūt saskaņā ar ES datu aizsardzības tiesību aktiem.

2.1. Kibernoturības panākšana

Lai veicinātu kibernoturību ES, valsts pārvaldes iestādēm un privātajam sektoram ir jāveido spējas un efektīvi jāsadarbojas. Balstoties uz pozitīvajiem rezultātiem, kas sasniegti ar līdz šim veiktajām darbībām[8], turpmāka ES rīcība var jo īpaši palīdzēt novērst kiberriskus un draudus, kuriem ir pārrobežu dimensija, un sniegt ieguldījumu saskaņotā reaģēšanā ārkārtas situācijās. Tas būs spēcīgs atbalsts iekšējā tirgus labai darbībai un uzlabos ES iekšējo drošību.

Eiropa paliks neaizsargāta, ja netiks pieliktas pamatīgas pūles publisko un privāto spēju, resursu un procedūru uzlabošanā kiberdrošības incidentu novēršanai, atklāšanai un risināšanai. Tāpēc Komisija ir izstrādājusi politiku attiecībā uz tīklu un informācijas drošību (TID)[9]. **Eiropas Tīklu un informācijas drošības aģentūra *ENISA*** tika nodibināta 2004. gadā[10], un Padome un Eiropas Parlaments apspriež jaunu regulu *ENISA* stiprināšanai un tās pilnvaru modernizēšanai[11]. Turklāt Pamatdirektīvā par elektronisko komunikāciju[12] noteikts, ka elektronisko komunikāciju pakalpojumu sniedzējiem pienācīgi jāpārvalda riski savos tīklos un jāpaziņo par būtiskiem drošības pārkāpumiem. ES datu aizsardzības tiesību aktos[13] arī noteikts, ka datu pārzinim jānodrošina datu aizsardzības prasību izpilde un garantijas, tostarp ar drošību saistīti pasākumi, un publiski pieejamu e-komunikāciju pakalpojumu jomā datu pārzinim ir jāpaziņo par incidentiem, kas ir saistīti ar personas datu aizsardzības pārkāpumu, kompetentajām valsts iestādēm.

Neraugoties uz panākumiem, ko veicinājušas brīvprātīgas saistības, ES joprojām pastāv trūkumi, jo īpaši saistībā ar valstu spējām, saskaņošanu pārrobežu incidentu gadījumos un privātā sektora iesaistīšanos un sagatavotību. Šai stratēģijai ir pievienots **tiesību akta** priekšlikums, lai jo īpaši:

- izveidotu kopīgas minimālas prasības attiecībā uz TID valsts līmenī, kas dalībvalstīm uzliktu šādus pienākumus: norīkot valsts kompetentās iestādes, kas atbild par TID, izveidot labi funkcionējošu *CERT* un pieņemt valsts TID stratēģiju un valsts TID sadarbības plānu. Spēju veidošana un saskaņošana attiecas arī uz ES iestādēm: 2012. gadā tika izveidota pastāvīga Datorapdraudējumu reaģēšanas vienība, kas atbild par ES iestāžu, aģentūru un struktūru IT sistēmu drošību („*CERT-EU*”).
- izveidotu saskaņotus novēršanas, atklāšanas, mazināšanas un reaģēšanas mehānismus, padarot iespējamu informācijas apmaiņu un savstarpēju palīdzību valstu TID kompetento iestāžu vidū. Valstu TID kompetento iestāžu uzdevums būs nodrošināt atbilstīgu ES mēroga sadarbību, jo īpaši uz Savienības TID sadarbības plāna pamata, kas izstrādāts, lai reaģētu uz kiberincidentiem ar pārrobežu dimensiju. Šī sadarbība tiks veidota arī uz

---

8 Sk. atsauces uz šo paziņojumu, kā arī Komisijas dienestu darba dokumentu – Ietekmes novērtējumu, kas pievienots Komisijas priekšlikumam direktīvai par tīklu un informācijas drošību, jo īpaši 4.1.4., 5.2. sadaļu, 2. pielikumu, 6. pielikumu, 8. pielikumu.

9 2001. gadā Komisija pieņēma paziņojumu „Tīklu un informācijas drošība — priekšlikums Eiropas politikas pieejai” (COM(2001) 298); 2006. gadā tā pieņēma Drošas informācijas sabiedrības stratēģiju (COM(2006) 251). Kopš 2009. gada Komisija ir arī pieņēmusi darbības plānu un paziņojumu par kritiskās infrastruktūras aizsardzību (*CIIP*) (COM(2009) 149, apstiprināts ar Padomes rezolūciju 2009/C 321/01, un COM(2011) 163, apstiprināts ar Padomes secinājumiem 10299/11)**.**

10 Regula (EK) Nr. 460/2004.

11 COM(2010)521. Šajā stratēģijā ierosinātās darbības nav saistītas ar *ENISA* esošo vai turpmāko pilnvaru grozīšanu.

12 Direktīvas 2002/21/EK 13.a un 13.b pants.

13 Direktīvas 95/46/EK 17. pants; Direktīvas 2002/58/EK 4. pants.

panākumu pamata, kas gūti Dalībvalstu Eiropas foruma (*EFMS*)[14] kontekstā, kurā ir notikušas produktīvas diskusijas un viedokļu apmaiņa par TID sabiedrisko politiku un kuru var integrēt sadarbības mehānismā, tiklīdz tāds tiks izveidots.

- uzlabotu privātā sektora sagatavotību un līdzdalību. Tā kā tīklu un informācijas sistēmu liela daļa pieder privātajam sektoram un privātais sektors nodrošina tās darbību, ciešāka sadarbība ar privāto sektoru ir būtiska kiberdrošības uzlabošanā. Privātajam sektoram tehniskā līmenī būtu jāveido savas kibernoturības spējas un jāapmainās ar paraugpraksi visās nozarēs. Rīkiem, kas nozarē izstrādāti reaģēšanai uz incidentiem, cēloņu noteikšanai un tiesu ekspertīzes veikšanai, vajadzētu būt pieejamiem arī publiskajam sektoram.

Tomēr privātajā sektorā joprojām nav efektīvu stimulu uzticamu datu par notikušiem TID incidentiem vai to ietekmi nodrošināšanai, riska pārvaldības kultūras veidošanai vai ieguldījumu veikšanai drošības risinājumos. Tādējādi ierosinātā tiesību akta mērķis ir nodrošināt, lai vairāku būtisku jomu (proti, enerģētika, transports, banku nozare, biržas un būtisku interneta pakalpojumu sniedzēji, kā arī valsts pārvaldes iestādes) dalībnieki novērtētu kiberdrošības riskus, ar kuriem tie saskaras, nodrošinātu tīklu un informācijas sistēmu uzticamību un noturību, izmantojot atbilstošu riska pārvaldību, un ziņotu par atklāto informāciju valstu TID kompetentajām iestādēm. Kiberdrošības kultūras izveide varētu palielināt uzņēmējdarbības iespējas un konkurenci privātajā sektorā, kurš varētu padarīt kiberdrošību par pārdodamu argumentu.

Šīm struktūrām vajadzētu ziņot valsts TID kompetentajām iestādēm par incidentiem, kuriem ir būtiska ietekme uz tādu pamata pakalpojumu un preču piegāžu nepārtrauktību, kuras ir atkarīgas no tīklu un informācijas sistēmām.

Valstu TID kompetentajām iestādēm būtu jāsadarbojas un jāapmainās ar informāciju ar citām regulatīvajām iestādēm un jo īpaši ar personas datu aizsardzības iestādēm. TID kompetentajām iestādēm savukārt būtu jāziņo tiesībaizsardzības iestādēm par incidentiem, ja radušās aizdomas par to nopietno kriminālo raksturu. Valstu kompetentajām iestādēm būtu arī regulāri jāpublicē (šim nolūkam paredzētā tīmekļa vietnē) neklasificēta informācija par aktuālajiem agrīnajiem brīdinājumiem par incidentiem un riskiem un par saskaņotu reaģēšanu. Juridiskiem pienākumiem nebūtu jāaizstāj vai jāliedz neformālas un brīvprātīgas sadarbības veidošana, tostarp starp publisko un privāto sektoru, lai palielinātu drošības līmeni un apmainītos ar informāciju un paraugpraksi. Eiropas publiskā un privātā sektora partnerība infrastruktūru noturības jautājumos (*EP3R*[15]) ir pamatota un derīga platforma ES līmenī, un ir jāturpina tās pilnveidošana.

Eiropas infrastruktūras savienošanas instruments (*CEF*)[16] nodrošinātu finansiālu atbalstu svarīgai infrastruktūrai, apvienojot dalībvalstu TID spējas un tādējādi atvieglojot sadarbību ES.

---

14 Dalībvalstu Eiropas forums tika izveidots ar COM(2009) 149 kā platforma diskusijas veicināšanai starp dalībvalstu publiskā sektora iestādēm par labu politikas praksi attiecībā uz informācijas kritiskās infrastruktūras drošību un noturību.

15 Eiropas publiskā un privātā sektora partnerība infrastruktūru noturības jautājumos tika izveidota ar COM(2009) 149. Ar šo platformu sākās darbs un tika veicināta sadarbība starp publisko un privāto sektoru saistībā ar būtisku aktīvu, resursu, funkciju un pamatprasību noteikšanu noturībai, kā arī sadarbības vajadzību un tādu mehānismu noteikšanai, kas palīdzētu reaģēt uz liela mēroga traucējumiem, kas ietekmē elektroniskās komunikācijas.

16 https://ec.europa.eu/digital-agenda/en/connecting-europe-facility. *CEF* budžeta pozīcija 09 03 02 – Telekomunikāciju tīkli (sekmēt valstu publisko tiešsaistes pakalpojumu starpsavienojumus un sadarbspēju, ka arī piekļuvi šādiem tīkliem).

Visbeidzot ārkārtīgi būtiskas ir kiberincidentu mācības ES līmenī, lai veicinātu sadarbību starp dalībvalstīm un privāto sektoru. Pirmās mācības, kurās iesaistījās dalībvalstis, tika īstenotas 2010. gadā („Kibereiropa 2010”), un otrās mācības, kurās piedalījās arī privātais sektors, notika 2012. gada oktobrī („Kibereiropa 2012”). ES un ASV teorētiskās mācības notika 2011. gada novembrī („Atlantiskās kibermācības 2011”). Turpmākas mācība tiek plānotas nākamajos gados, tostarp ar starptautiskiem partneriem.

Komisija apņemas:

- turpināt savas darbības, ko veic Kopīgais pētniecības centrs ciešā sadarbībā ar dalībvalstu iestādēm un kritisko infrastruktūru īpašniekiem un apsaimniekotājiem attiecībā uz Eiropas kritiskās infrastruktūras TID vājo vietu noteikšanu un noturīgu sistēmu attīstības veicināšanu;
- 2013. gada sākumā sākt ES finansētu izmēģinājuma projektu[17] par **cīņu pret robottīkliem un ļaunprātīgu programmatūru**, lai nodrošinātu koordinācijas un saskaņošanas sistēmu starp ES dalībvalstīm, privātā sektora organizācijām, piemēram, interneta pakalpojumu sniedzējiem, un starptautiskiem partneriem.

Komisija aicina *ENISA*:

- palīdzēt dalībvalstīm veidot stipras **valsts kibernoturības spējas**, jo īpaši pilnveidojot zināšanas par nozares kontroles sistēmu, transporta un enerģētikas infrastruktūras drošību un noturību;
- 2013. gadā izpētīt nozares kontroles sistēmu datoru drošības incidentu vienības(-u) (*ICS-CSIRT*) īstenošanas iespējas ES;
- turpināt atbalstīt dalībvalstis un ES iestādes regulāru **Eiropas kiberincidentu mācību** īstenošanā, kuras arī veidos operatīvo bāzi ES līdzdalībai starptautiskās kiberincidentu mācībās.

Komisija aicina Eiropas Parlamentu un Padomi:

- ātri **pieņemt** priekšlikumu direktīvai par **vienādi augsta līmeņa tīklu un informācijas drošību (TID)** visā Savienībā, kurā risināti jautājumi saistībā ar valstu spējām un sagatavotību, ES līmeņa sadarbību, riska pārvaldības prakses ieviešanu un informācijas apmaiņu par TID.

Komisija aicina nozari:

- uzņemties vadību **ieguldījumu veikšanā** augta līmeņa kiberdrošībā un attīstīt paraugprakses un informācijas apmaiņu sektoru līmenī, kā arī ar publiskām iestādēm, lai nodrošinātu aktīvu un personu stipru un efektīvu aizsardzību, jo īpaši ar tādu publiskā un privātā sektora partnerību starpniecību kā *EP3R* un „Uzticība digitālajai dzīvei” (*TDL*)[18].

[17] CIP-ICT PSP-2012-6, 325188. Tā kopējais budžets ir 15 miljoni euro, un ES finansējums veido 7,7 miljonus euro.

[18] http://www.trustindigitallife.eu/.

Izpratnes veicināšana

Kiberdrošības garantēšana ir kopīga atbildība. Lietotājiem ir būtiska loma tīklu un informācijas sistēmu drošības nodrošināšanā, un ir jāveicina viņu izpratne par riskiem, ar kuriem viņi saskaras tiešsaistē, un spēja veikt vienkāršas darbības, lai pasargātu sevi no tiem.

Pēdējos gados ir izstrādātas vairākas iniciatīvas, un tās ir jāturpina. Konkrēti, *ENISA* ir iesaistījusies izpratnes veicināšanā, publicējot ziņojumus, organizējot ekspertu seminārus un veidojot publiskā un privātā sektora partnerības. Eiropols, *Eurojust* un valstu datu aizsardzības iestādes arī aktīvi nodarbojas ar izpratnes veicināšanu. *ENISA* un dažas dalībvalstis 2012. gada oktobrī izmēģinājuma kārtā organizēja Eiropas kiberdrošības mēnesi. Izpratnes veicināšana ir viena no jomām, kuru attīsta ES un ASV darba grupa kiberdrošības un kibernoziedzības jautājumos[19], un tā ir būtiska programmas „Drošāks internets"[20] (kas ir vērsta uz bērnu drošību tiešsaistē) kontekstā.

Komisija aicina *ENISA*:

- 2013. gadā ierosināt ceļvedi brīvprātīgai sertifikācijas programmai „Tīklu un informācijas drošības apliecība", kas veicinātu IT speciālistu (piemēram, tīmekļa vietņu administratoru) prasmju un zināšanu uzlabošanu.

Komisija apņemas:

- ar *ENISA* atbalstu 2014. gadā organizēt kiberdrošības **konkursu**, kurā TID risinājumus piedāvātu un sacenstos augstskolu studenti.

Komisija aicina dalībvalstis[21]:

- ar *ENISA* atbalstu, iesaistot arī privāto sektoru, no 2013. gada organizēt ikgadēju **kiberdrošības mēnesi**, kura mērķis ir veicināt izpratni lietotāju vidū. ES un ASV kiberdrošības mēnesis tiks vienlaikus organizēts 2014. gadā;
- **palielināt valstu devumu TID izglītībā un apmācībā**, ieviešot TID apmācību skolās līdz 2014. gadam, apmācību par TID un drošas programmatūras izstrādi un personas datu aizsardzību datorzinātņu studentiem, ka arī TID pamata apmācību personālam, kas strādā valsts pārvaldē.

Komisija aicina nozari:

- veicināt **izpratni** par kiberdrošību **visos līmeņos** gan uzņēmējdarbības praksē, gan saskarsmē ar klientiem. Konkrēti, nozares pārstāvjiem būtu jāapsver veidi, kā palielināt izpilddirektoru un padomju atbildību par kiberdrošību.

---

19 Šai darba grupai, kas tika izveidota ES un ASV augstākā līmeņa sanāksmē 2010. gada novembrī (MEMO/10/597), ir dots uzdevums izstrādāt kopīgas pieejas daudzos kiberdrošības un kibernoziedzības jautājumos.

20 Programma „Drošāks internets" finansē sabiedrisko organizāciju sadarbības tīklu, kas aktīvi darbojas bērnu interešu tiešsaistē jomā, tiesībaizsardzības iestāžu sadarbības tīklu, kuras apmainās ar informāciju un paraugpraksi saistībā ar interneta izmantošanu noziedzīgos nolūkos, izplatot bērnu seksuālas izmantošanas materiālus, un pētnieku sadarbības tīklu, kas vāc informāciju par tiešsaistes tehnoloģiju izmantojumu, tā riskiem un sekām bērnu dzīvē.

21 Iesaistot arī attiecīgas valsts pārvaldes iestādes, tostarp TID kompetentās iestādes un datu aizsardzības iestādes.

2.2. Kibernoziedzības būtiska samazināšana

Jo digitalizētāka kļūst mūsu pasaule, jo vairāk iespēju rodas kibernoziedzniekiem. Kibernoziedzība ir viena no noziedzības formām, kas pieaug visstraujāk, un ik dienu par tās upuriem kļūst vairāk nekā miljons cilvēku. Kibernoziedznieki un kibernoziedzības tīkli kļūst arvien prasmīgāki, un mums ir vajadzīgi piemēroti operatīvi rīki un spējas, lai vērstos pret tiem. Kibernoziegumi nes lielu peļņu un ir saistīti ar zemu risku, un noziedznieki bieži izmanto tīmekļa vietņu domēnu anonimitāti. Kibernoziegumi tiek veikti pāri robežām – interneta pieejamība visā pasaulē nozīmē, ka tiesībaizsardzības iestādēm jāizmanto saskaņota un uz sadarbību balstīta pārrobežu pieeja, lai reaģētu uz šiem arvien pieaugošajiem draudiem.

Stingri un efektīvi tiesību akti

ES un dalībvalstīm ir vajadzīgi stingri un efektīvi tiesību akti, lai cīnītos ar kibernoziedzību. Eiropas Padomes Konvencija par kibernoziedzību, kas pazīstama arī kā Budapeštas konvencija, ir saistošs starptautisks nolīgums, kurš sniedz efektīvu pamatu valsts tiesību aktu pieņemšanai.

ES jau ir pieņēmusi tiesību aktus par kibernoziedzību, tostarp Direktīvu par bērnu seksuālas izmantošanas tiešsaistē un bērnu pornogrāfijas apkarošanu[22]. ES arī plāno vienoties par direktīvu par uzbrukumiem informācijas sistēmām, kas tiek veikti, īpaši izmantojot robottīklus.

Komisija apņemas:

- nodrošināt direktīvu, ka attiecas uz kibernoziedzību, ātru transponēšanu un īstenošanu;
- mudināt dalībvalstis, kas vēl nav ratificējušas **Eiropas Padomes Budapeštas konvenciju par kibernoziedzību**, to ratificēt un īstenot tās noteikumus pēc iespējas ātri.

Uzlabotas operatīvās spējas cīnīties pret kibernoziedzību

Kibernoziedzības metodes ir strauji pilnveidojušās – tiesībaizsardzības iestādes nespēj cīnīties pret kibernoziedzību ar novecojušiem operatīviem instrumentiem. Pašlaik ne visām dalībvalstīm ir nepieciešamā operatīvā spēja, lai efektīvi reaģētu uz kibernoziedzību. Visām dalībvalstīm ir vajadzīgas efektīvas valsts kibernoziedzības apkarošanas vienības.

Komisija apņemas:

- ar finansēšanas programmu[23] palīdzību palīdzēt dalībvalstīm **noteikt trūkumus un stiprināt to spējas** izmeklēt kibernoziegumus un cīnīties pret tiem. Komisija turklāt atbalstīs struktūras, kas veido saikni starp pētniekiem/akadēmiskajām aprindām, tiesībaizsardzības iestāžu darbiniekiem un privāto sektoru – līdzīgi kā to pašlaik dara Komisijas finansētie kibernoziedzības apkarošanas izcilības centri,

[22] Direktīva 2011/93/ES, ar kuru aizstāj Padomes pamatlēmumu 2004/68/TI.

[23] 2013. gadā saskaņā ar īpašu programmu „Noziedzības profilakse un apkarošana" (*ISEC*). Pēc 2013. gada saskaņā ar Iekšējās drošības fondu (jauns instruments atbilstīgi jaunajai daudzgadu finanšu shēmai).

kas izveidoti dažās dalībvalstīs;

- kopā ar dalībvalstīm koordinēt centienus apzināt paraugpraksi un labākās pieejamās metodes, tostarp ar Kopīgā pētniecības centra palīdzību, cīņai pret kibernoziedzību (piemēram, attiecībā uz tiesu ekspertīzes rīku izstrādi un izmantošanu vai attiecībā uz draudu analīzi);
- cieši sadarboties ar nesen izveidoto **Eiropas Kibernoziedzības centru (*EC3*) Eiropolā un ar *Eurojust***, lai saskaņotu šādas politikas pieejas ar paraugpraksi operatīvajā jomā.

Labāka koordinācija ES līmenī

ES var sniegt savu ieguldījumu dalībvalstu darbā, atvieglojot koordinētas un uz sadarbību balstītas pieejas izmantošanu, kas ļauj apvienot tiesībaizsardzības iestādes un tiesu iestādes, kā arī publiskā un privātā sektora ieinteresētās personas no ES un ārpus tās.

Komisija apņemas:

- atbalstīt nesen izveidoto **Eiropas Kibernoziedzības centru** (*EC3*), kas ir Eiropas koordinācijas iestāde cīņā pret kibernoziedzību. *EC3* nodrošinās analīzi un izlūkošanu, atbalstīs izmeklēšanu, nodrošinās augsta līmeņa tiesu ekspertīzi, atvieglos sadarbību, veidos informācijas apmaiņas kanālus starp kompetentajām iestādēm dalībvalstīs, privāto sektoru un citām ieinteresētajām personām un pakāpeniski kļūs par tiesībaizsardzības iestāžu ruporu[24];
- atbalstīt centienus domēnu nosaukumu reģistrētāju atbildības palielināšanā un nodrošināt informācijas pareizību par tīmekļa vietņu īpašniekiem, jo īpaši pamatojoties uz Piešķirto nosaukumu un numuru interneta korporācijai (*ICANN*) sniegtajiem tiesībaizsardzības ieteikumiem saskaņā ar Savienības tiesību aktiem, tostarp noteikumiem par datu aizsardzību;
- balstoties uz nesen pieņemtajiem tiesību aktiem, turpināt stiprināt ES centienus cīnīties pret bērnu seksuālo izmantošanu tiešsaistē. Komisija ir pieņēmusi Eiropas stratēģiju „Bērniem labāks internets”[25] un kopā ar ES valstīm un valstīm, kas atrodas ārpus ES, izveidojusi Pasaules aliansi pret seksuālu vardarbību pret bērniem tiešsaistē[26]. Alianse ir līdzeklis dalībvalstu turpmāko darbību īstenošanai, kuras atbalsta Komisija un *EC3*.

Komisija aicina Eiropolu (*EC3*):

- sākotnēji koncentrēt savu analītisko un operatīvo atbalstu uz dalībvalstu kibernoziegumu izmeklēšanu, lai palīdzētu sagraut kibernoziedznieku tīklus, kas darbojas galvenokārt tādās jomās kā bērnu seksuālā izmantošana, maksājumu krāpniecība, robottīkli un kiberielaušanās;

[24] 2012. gada 28. martā Eiropas Komisija pieņēma paziņojumu „Vēršanās pret noziedzību mūsu digitālajā laikmetā: Eiropas Kibernoziedzības centra izveide”.

[25] COM(2012) 196 galīgā redakcija.

[26] Padomes 2012. gada 7. un 8. jūnija secinājumi par Pasaules aliansi pret seksuālu vardarbību pret bērniem tiešsaistē (ES un ASV kopīgais paziņojums) un Deklarācija par Pasaules alianses pret seksuālu vardarbību pret bērniem tiešsaistē izveidi (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm).

- regulāri sagatavot stratēģiskus un darbības pārskatus par tendencēm un jauniem apdraudējumiem, lai noteiktu prioritātes un kibernoziegumu izmeklēšanas vienību darbības virzienu dalībvalstīs.

Komisija aicina Eiropas Policijas akadēmiju (*CEPOL*) sadarbībā ar Eiropolu:

- koordinēt mācību kursu izstrādi un plānošanu, lai nodrošinātu tiesībaizsardzības darbiniekiem vajadzīgās zināšanas un kompetenci iedarbīgai cīņai ar kibernoziegumiem.

Komisija aicina *Eurojust*:

- konstatēt galvenos šķēršļus, kas apgrūtina tiesu sadarbību kibernoziegumu izmeklēšanā un koordināciju starp dalībvalstīm un ar trešām valstīm, un atbalstīt kibernoziegumu izmeklēšanu un kriminālvajāšanu gan operatīvā, gan stratēģiskā līmenī, kā arī atbalstīt mācību pasākumus šajā jomā.

Komisija aicina *Eurojust* un Eiropolu (*EC3*):

- cieši sadarboties saskaņā ar to attiecīgajām pilnvarām un kompetenci, arī izmantojot informācijas apmaiņu, lai palielinātu kibernoziegumu apkarošanas iedarbīgumu.
-

2.3. Kiberaizsardzības politikas izstrāde un spēju veidošana saistībā ar kopējo drošības un aizsardzības politiku (KDAP)

Kiberdrošības pasākumi Eiropas Savienībā ietver arī kiberaizsardzības dimensiju. Lai palielinātu tādu komunikācijas un informācijas sistēmu noturību, kas atbalsta dalībvalstu aizsardzības un valsts drošības intereses, kiberaizsardzības spēju veidošana jākoncentrē uz sarežģītu kiberdraudu konstatēšanu, reaģēšanu uz šādiem draudiem un darbības atjaunošanu pēc šādiem draudiem.

Ņemot vērā, ka draudi ir daudzveidīgi, svarīgāko kiberobjektu aizsardzībā ir jāpastiprina sinerģija starp civilo un militāro pieeju. Šie centieni ir jāatbalsta ar pētniecību un izstrādi un ar ciešāku sadarbību starp valdībām, privāto sektoru un akadēmiskajām aprindām Eiropas Savienībā. Lai novērstu dublēšanos, ES pētīs iespējas, kā ES un NATO var papildināt savus pūliņus, kas tiek pielikti, lai uzlabotu tādu valdības, aizsardzības un citu svarīgāko informācijas infrastruktūras objektu noturību, no kuriem atkarīgi abu organizāciju dalībnieki.

Augstā pārstāve galveno uzmanību pievērsīs šādām svarīgākajām darbībām un aicinās dalībvalstis un Eiropas Aizsardzības aģentūru sadarboties šādā ziņā:

- novērtēt ES kiberaizsardzības prasības un veicināt ES kiberaizsardzības potenciāla un tehnoloģiju attīstību, lai pievērstos visiem spēju veidošanas aspektiem, ieskaitot politisko programmu, vadību, organizāciju, personālu, apmācību, tehnoloģijas, infrastruktūru, loģistiku un sadarbspēju;

- izstrādāt ES kiberaizsardzības politikas satvaru, lai aizsargātu tīklus KADP misijās un operācijās, ieskaitot dinamisko riska vadību, draudu labāku analīzi un informācijas apmaiņu. Uzlabot kiberaizsardzības mācību un prakses iespējas militārpersonām Eiropas

un daudznacionālā kontekstā, ieskaitot kiberaizsardzības elementu integrēšanu pašreizējos prakses katalogos;

- veicināt dialogu un koordināciju starp civilās sabiedrības un militārajām aprindām Eiropas Savienībā, liekot īpašu uzsvaru uz paraugprakses apmaiņu, informācijas apmaiņu un agrīno brīdināšanu, reaģēšanu uz incidentiem, riska novērtēšanu, izpratnes veicināšanu un kiberdrošības noteikšanu par prioritāti;

- izveidot dialogu ar starptautiskajiem parteriem, tostarp NATO, citām starptautiskajām organizācijām un daudznacionālajiem izcilības centriem, lai nodrošinātu aizsardzības potenciālu, noteiktu sadarbības jomas un novērstu centienu dublēšanos.

2.4. Rūpniecisko un tehnoloģisko resursu veidošana kiberdrošības vajadzībām

Eiropai ir izcilas pētniecības un izstādes iespējas, taču daudzi no pasaules līderiem, kas piedāvā inovatīvus IKT produktus un pakalpojumus, atrodas ārpus ES. Pastāv risks, ka Eiropa ne tikai kļūs pārmērīgi atkarīga no citviet ražotām informācijas un komunikācijas tehnoloģijām, bet arī no drošības risinājumiem, kas izstrādāti ārpus tās robežām. Ir būtiski nodrošināt, ka aparatūras un programmatūras komponenti, kas ražoti ES un trešās valstīs un kas tiek izmantoti svarīgākajos pakalpojumos un infrastruktūrā un arvien vairāk arī pārnēsājamās ierīcēs, ir uzticami, droši un garantē personas datu aizsardzību.

Kiberdrošības produktu vienotā tirgus veicināšana

Augstu drošības līmeni var garantēt tikai tad, ja drošība ir prioritāte visiem vērtības ķēdes dalībniekiem (piemēram, iekārtu ražotājiem, programmatūras izstrādātajiem, informācijas sabiedrības pakalpojumu sniedzējiem). Tomēr šķiet[27], ka daudzi iesaistītie dalībnieki uzskata drošību par papildu apgrūtinājumu, un pieprasījums pēc drošības risinājumiem nav liels. Ir jābūt atbilstošām kiberdrošības veiktspējas prasībām, kas tiek īstenotas visā Eiropā izmantoto IKT produktu vērtības ķēdē. Privātajam sektoram ir vajadzīgi stimuli, lai nodrošinātu augstu kiberdrošības līmeni; piemēram, marķējumi, kas norāda adekvātu kiberdrošības veiktspēju, dos iespēju uzņēmumiem ar labu kiberdrošības veiktspēju un vēsturi akcentēt to savā pārdošanas stratēģijā un tādējādi gūt konkurences priekšrocības. Arī pienākumi, kas izklāstīti ierosinātajā TID direktīvā, būtiski palīdzētu palielināt uzņēmumu konkurētspēju attiecīgajās nozarēs.

Ir jāstimulē arī Eiropas mēroga tirgus pieprasījums pēc ražojumiem ar augstu drošības līmeni. Pirmkārt, šīs stratēģijas mērķis ir palielināt sadarbību un pārredzamību par IKT ražojumu drošību. Tajā ir pausts aicinājums izveidot platformu, kura apvienotu attiecīgās Eiropas publiskā sektora un privātā sektora ieinteresētās aprindas, lai identificētu kiberdrošības paraugpraksi visā vērtības ķēdē un radītu labvēlīgus tirgus apstākļus drošu IKT risinājumu izstrādei un pieņemšanai. Uzmanības centrā būs radīt stimulus piemērotas riska vadības īstenošanai un pieņemt drošības standartus un risinājumus, kā arī, iespējams, izveidot brīvprātīgas ES mēroga sertifikācijas sistēmas, kas balstās uz pašreizējām ES un starptautiskajām sistēmām. Komisija veicinās konsekventu pieeju pieņemšanu dalībvalstīs, lai novērstu atšķirības, kas uzņēmumiem rada ar atrašanās vietu saistītus trūkumus.

Otrkārt, Komisija atbalstīs drošības standartu izstrādi un palīdzēs izveidot ES mēroga brīvprātīgas sertifikācijas sistēmas mākoņdatošanas jomā, vienlaikus pienācīgi ņemot vērā

[27] Sk. 4.1.5.2. punktu Komisijas dienestu darba dokumentā – Ietekmes novērtējumā, kas pievienots Komisijas priekšlikumam Direktīvai par tīklu un informācijas drošību.

nepieciešamību nodrošināt datu aizsardzību. Darbam būtu jākoncentrējas uz piegādes ķēdes drošību, jo īpaši svarīgākajās tautsaimniecības nozarēs (rūpnieciskas kontroles sistēmas, enerģētikas un transporta infrastruktūra). Šādam darbam jābalstās uz pašreizējo standartizācijas darbu, ko veic Eiropas standartizācijas organizācijas (*CEN*, *CENELEC* un *ETSI*)[28], Kiberdrošības koordinācijas grupa (*CSCG*), kā arī uz *ENISA*, Komisijas un citu saistīto dalībnieku kompetenci.

Komisija apņemas:

- 2013. gadā uzsākt publiskā un privātā sektora **platformu TID risinājumiem**, lai izstrādātu stimulus drošu IKT risinājumu pieņemšanai un labas kiberdrošības veiktspējas ieviešanai attiecībā uz visā Eiropā izmantojamiem IKT ražojumiem;
- 2014. gadā ierosināt ieteikumus, lai nodrošinātu kiberdrošību visā IKT vērtības ķēdē, pamatojoties uz minētās platformas darbu;
- izpētīt, kā lielākie IKT aparatūras un programmatūras nodrošinātāji varētu informēt valstu kompetentās iestādes par konstatētajām nepilnībām, kam varētu būt nopietnas sekas drošībai.

Komisija aicina *ENISA*:

- sadarbībā ar attiecīgajām valstu kompetentajām iestādēm, ieinteresētajām personām, starptautiskajām un Eiropas standartizācijas iestādēm un Eiropas Komisijas Kopīgo pētniecības centru izstrādāt **tehniskas vadlīnijas un ieteikumus TID standartu un paraugprakses pieņemšanai** publiskajā un privātajā sektorā.

Komisija aicina publiskā un privātā sektora ieinteresētās aprindas:

- veicināt to, lai IKT produktu ražotāji un pakalpojumu sniedzēji, tostarp mākoņdatošanas pakalpojumu sniedzēji, izstrādātu un pieņemtu rūpniecības nozares virzītus **drošības standartus**, tehniskās normas un integrētas drošības un integrēta privātuma principus; jaunas paaudzes programmatūrai un aparatūrai jābūt aprīkotai ar **pamatīgākiem, iekļautiem un lietotājam ērtiem drošības elementiem**;
- izstrādāt rūpniecības nozares virzītus standartus attiecībā uz uzņēmumu veiktspēju kiberdrošības jomā un uzlabot sabiedrībai pieejamo informāciju, izstrādājot **drošības marķējumu** vai drošības zīmes, kas palīdzētu patērētājiem izdarīt savu izvēli.

Ieguldījumus pētniecībā, izstrādē un inovācijā veicināšana

Pētniecība un izstrāde var atbalstīt spēcīgu rūpniecisko politiku, veicināt Eiropas IKT nozares uzticamību, stimulēt iekšējo tirgu un samazināt Eiropas atkarību no ārzemju tehnoloģijām. Pētniecībai un izstrādei ir jāaizpilda tehnoloģiskās nepilnības IKT drošības jomā, jāsagatavojas nākamās paaudzes drošības problēmu risināšanai, jāņem vērā lietotāju vajadzību nepārtrauktā evolūcija un jāizmanto divējāda lietojuma tehnoloģiju sniegtās priekšrocības.

[28] Jo īpaši saskaņā ar Viedo tīklu standartu M/490 attiecībā uz pirmo standartu kopumu viedo tīklu un etalonarhitektūras jomā.

Pētniecībai un izstrādei būtu jāturpina atbalstīt arī kriptogrāfijas attīstību. Tas ir jāpapildina ar centieniem pārvērst pētniecības un izstrādes rezultātus komerciālos risinājumos, sniedzot vajadzīgos stimulus un ieviešot piemērotus apstākļus no politikas izstrādes viedokļa.

Eiropas Savienībai ir iespējami labāk jāizmanto Pētniecības un inovācijas pamatprogramma "Apvārsnis 2020"[29], ko paredzēts uzsākt 2014. gadā. Komisijas priekšlikumā ir iekļauti konkrēti mērķi uzticamām IKT, kā arī kibernoziegumu apkarošanai, kas ir saskaņā ar šo stratēģiju. "Apvārsnis 2020" atbalstīs drošības pētniecību, kas saistīta ar jaunajām IKT tehnoloģijām, sniegs risinājumus viscaur drošu IKT sistēmu, pakalpojumu un lietotņu vajadzībām, nodrošinās stimulus pašlaik pieejamo risinājumu īstenošanai un pieņemšanai un pievērsīsies tīklu un informācijas sistēmu sadarbspējai. Īpaša uzmanība ES līmenī tiks pievērsta tam, lai optimizētu un labāk koordinētu dažādas finansējuma programmas ("Apvārsnis 2020", Iekšējās drošības fonds, Eiropas Aizsardzības aģentūras veikta pētniecība, ieskaitot Eiropas sadarbības sistēmu).

Komisija apņemas:

- izmantot pamatprogrammu "Apvārsnis 2020", lai risinātu virkni jautājumu IKT privātuma un drošības jomā, no pētniecības un izstrādes līdz inovācijām un izvēršanai. "Apvārsnis 2020" turklāt izstrādās rīkus un instrumentus cīņai ar kriminālām un teroristu darbībām, kas vērstas uz kibervidi;
- izveidot mehānismus labākai Eiropas Savienības iestāžu un dalībvalstu pētniecības dienaskārtības koordinācijai un radīt stimulus dalībvalstīm vairāk līdzekļu ieguldīt pētniecībā un izstrādē.

Komisija aicina dalībvalstis:

- līdz 2013. gada beigām izstrādāt paraugpraksi, lai izmantotu **valsts pārvaldes iestāžu pirktspēju** (piemēram, izmantojot publisko iepirkumu) tam, lai stimulētu IKT produktu un pakalpojumu drošības elementu izstrādi un ieviešanu;
- veicināt rūpniecības un akadēmisko aprindu agrīnu iesaistīšanos risinājumu izstrādē un koordinācijā. Tas būtu jādara, iespējami pilnvērtīgāk izmantojot Eiropas rūpniecisko bāzi un saistītās pētniecības un izstrādes tehnoloģiskās inovācijas un koordinējot civilo un militāro organizāciju pētniecības dienaskārtību.

Komisija aicina Eiropolu un *ENISA*:

- noteikt jaunas tendences un vajadzības, ņemot vērā arvien mainīgos kibernoziegumu un kiberdrošības modeļus, lai izstrādātu adekvātus digitālās tiesu ekspertīzes rīkus un tehnoloģijas.

Komisija aicina publiskā un privātā sektora ieinteresētās aprindas:

- sadarbībā ar apdrošināšanas nozari izstrādāt **harmonizētu mērvienību sistēmu riska prēmiju aprēķināšanai**, kas dotu iespēju uzņēmumiem, kuri ir veikuši ieguldījumus drošībā, maksāt zemāka riska prēmijas.

[29] "Apvārsnis 2020" ir finanšu instruments, ar kuru īsteno stratēģijas "**Eiropa 2020**" pamatiniciatīvu "**Inovācijas Savienība**", kuras mērķis ir nodrošināt Eiropas konkurētspēju pasaules mērogā. ES jaunā pētniecības un inovācijas pamatprogramma, kas darbosies no 2014. līdz 2020. gadam, būs viens no virzītājspēkiem jaunas izaugsmes un darbvietu radīšanai Eiropā.

2.5. Saskaņōtas starptautiskas kibertelpas politikas izveide Eiropas Savienībā un ES pamatvērtību popularizēšana

Atvērtas, brīvas un drošas kibertelpas saglabāšana ir globāls izaicinājums, kas Eiropas Savienībai ir jārisina kopā ar attiecīgajiem starptautiskajiem partneriem un organizācijām, privāto sektoru un pilsonisko sabiedrību.

Savā starptautiskajā kibertelpas politikā ES centīsies veicināt interneta atvērtību un brīvību, sekmēt centienus izstrādāt uzvedības normas un piemērot pašreizējos starptautiskos tiesību aktus kibertelpai. ES strādās arī pie tā, lai mazinātu digitālo plaisu, un aktīvi piedalīsies starptautiskos pasākumos, kas vērsti uz kiberdrošības spēju veidošanu. ES starptautiskā līdzdalība kiberjautājumu risināšanā notiks saskaņā ar ES pamatvērtībām – cilvēka cieņu, brīvību, demokrātiju, vienlīdzību, tiesiskumu un pamattiesību ievērošanu.

Kiberjautājumu integrēšana ES arējās attiecībās un kopējā ārpolitikā un drošības politikā

Komisijai, Augstajai pārstāvei un dalībvalstīm būtu jāpauž saskaņota ES starptautiskā kibertelpas politika, kuras mērķis ir panākt lielāku svarīgāko starptautisko partneru un organizāciju līdzdalību un ciešākas attiecības ar šiem partneriem un organizācijām, kā arī ar pilsonisko sabiedrību un privāto sektoru. ES konsultācijām ar starptautiskajiem partneriem kiberjautājumu jomā jābūt plānotām, koordinētām un īstenotām tā, lai pievienotu vērtību pašreizējam divpusējam dialogam starp ES dalībvalstīm un trešām valstīm. ES liks atjaunotu akcentu uz dialogu ar trešām valstīm, īpaši pievēršoties līdzīgi domājošiem partneriem, kam ar ES ir kopīgas vērtības. Tā tieksies panākt augsta līmeņa datu aizsardzību, arī attiecībā uz privāto datu nodošanu trešām valstīm. Lai risinātu globālās problēmas kibertelpā, ES centīsies panākt ciešāku sadarbību ar organizācijām, kas darbojas šajā jomā, tādām kā Eiropas Padome, ESAO, ANO, EDSO, NATO, Āfrikas Savienība, Dienvidaustrumāzijas valstu asociācija un Amerikas valstu organizācija. Divpusējā līmenī sadarbība ar Amerikas Savienotajām Valstīm ir īpaši svarīga un tiks attīstīta turpmāk, konkrēti, izmantojot ES un ASV darba grupu kiberdrošības un kibernoziedzības jautājumos.

Viens no svarīgākajiem elementiem ES starptautiskajā kiberpolitikā būs veicināt kibertelpu kā brīvības un pamattiesību telpu. Plašākai piekļuvei internetam būtu jāveicina un jāatbalsta demokrātiskas reformas visā pasaulē. Aizvien plašākai globālai savienojamībai nevajadzētu būt saistītai ar cenzūru vai masu uzraudzību. ES būtu jāveicina korporatīva sociālā atbildība[30] un jāuzsāk starptautiskas iniciatīvas globālās koordinācijas uzlabošanai šajā jomā.

Atbildība par drošāku kibertelpu jāuzņemas visiem globālās informācijas sabiedrības locekļiem, sākot ar iedzīvotājiem un beidzot ar valdībām. ES atbalsta centienus noteikt kibertelpā uzvedības normas, kuras būtu jāievēro visām ieinteresētajām personām. ES arī sagaida, ka, tāpat kā iedzīvotāji tiešsaistē pilda pilsoniskos pienākumus, uzņemas sociālo atbildību un ievēro likumus, arī valstīm būtu jāievēro noteiktas normas un spēkā esošie tiesību akti. Attiecība uz starptautiskās drošības jautājumiem ES mudina izstrādāt pasākumus uzticēšanās gaisotnes radīšanai kiberdrošības jomā, palielināt pārredzamību un samazināt pārpratumu risku valstu attiecībās.

ES neaicina radīt jaunu starptautisku tiesību instrumentu, kas reglamentētu kiberjautājumus.

---

[30] Atjaunota ES stratēģija 2011.–2014. gadam attiecībā uz korporatīvo sociālo atbildību; COM(2011) 681 galīgā redakcija.

Juridiskās saistības, kas ietvertas Starptautiskajā paktā par pilsoniskajām un politiskajām tiesībām, Eiropas Cilvēktiesību konvencijā un ES Pamattiesību hartā, ir jāpilda arī tiešsaistes vidē. ES galveno uzmanību pievērsīs tam, kā nodrošināt šo pasākumu īstenošanu arī kibervidē.

Lai vērstos pret kibernoziedzību, Budapeštas konvencija ir instruments, kas atvērts pieņemšanai trešajās valstīs. Tā kalpo par paraugu valsts tiesību aktu izstrādei kibernoziedzības jomā un par pamatu starptautiskajai sadarbībai šajā jomā.

Ja bruņoti konflikti paplašinās uz kibervidi, attiecīgajā gadījumā tiks piemērotas starptautiskās humanitārās tiesības un vajadzības gadījumā cilvēktiesības. **Spēju kiberdrošības jomā un noturīgu informācijas infrastruktūru veidošana trešās valstīs**

To infrastruktūru, kas nodrošina un veicina komunikācijas pakalpojumus, raitai darbībai starptautiska sadarbība nāks par labu. Tā ietver apmaiņu ar paraugpraksi, informācijas apmaiņu, kopīgus agrīnas brīdināšanas pārbaudījumus incidentu pārvaldībā un tamlīdzīgas darbības. ES virzīsies uz šo mērķi, aktīvāk piedaloties notiekošajos starptautiskajos pasākumos ar mērķi nostiprināt sadarbības tīklus, kuros iesaistītas valdības un privātais sektors, informācijas kritiskās infrastruktūras aizsardzībai (*CIIP*).

Nebūt ne visur pasaulē var izmantot interneta sniegtās priekšrocības, jo trūkst atvērtas, drošas, sadarbspējīgas un uzticamas piekļuves. Tādēļ Eiropas Savienība turpinās atbalstīt valstu centienus padarīt internetu pieejamāku saviem iedzīvotājiem un paplašināt lietotāju loku, nodrošināt tā integritāti un drošumu un efektīvi apkarot kibernoziedzību.

Sadarbībā ar dalībvalstīm Komisija un Augstā pārstāve

- strādās pie saskaņotas ES starptautiskas kibertelpas politikas, lai pastiprinātu sadarbību ar galvenajiem starptautiskajiem partneriem un organizācijām, iekļautu kiberjautājumus KĀDP un uzlabotu globālu kiberjautājumu koordināciju;
- atbalstīs uzvedības normu izstrādi un uzticības veicināšanas pasākumus kiberdrošības jomā; sekmēs dialogus par to, kā piemērot spēkā esošās starptautisko tiesību normas kibertelpas jomā un veicināt Budapeštas konvencijas piemērošanu, vēršoties pret kibernoziedzību;
- atbalstīs pamattiesību, tostarp piekļuves informācijai un vārda brīvības, piemērošanu un aizsardzību, īpašu uzmanību pievēršot šādiem aspektiem: a) izstrādāt jaunas publiskās vadlīnijas par vārda brīvību tiešsaistē un bezsaistē; b) pārraudzīt to produktu vai pakalpojumu eksportu, kurus varētu izmantot cenzūrai vai masu uzraudzībai tiešsaistē; c) izstrādāt pasākumus un rīkus nolūkā palielināt piekļuvi internetam, tā atvērtību un noturību, lai vērstos pret komunikācijas tehnoloģiju īstenotu cenzūru vai masu uzraudzību; d) dot iespēju dalībniekiem izmantot komunikācijas tehnoloģijas pamattiesību piemērošanai;
- sadarboties ar starptautiskajiem partneriem un organizācijām, privāto sektoru un pilsonisko sabiedrību, lai atbalstītu globālu spēju veidošanu trešās valstīs ar mērķi uzlabot piekļuvi informācijai un atvērtam internetam, lai nepieļautu kiberdraudus, kibernoziegumus un kiberterorismu un vērstos pret tiem, tostarp nejaušiem gadījumiem, un lai nodrošinātu līdzekļu devēju koordināciju nolūkā

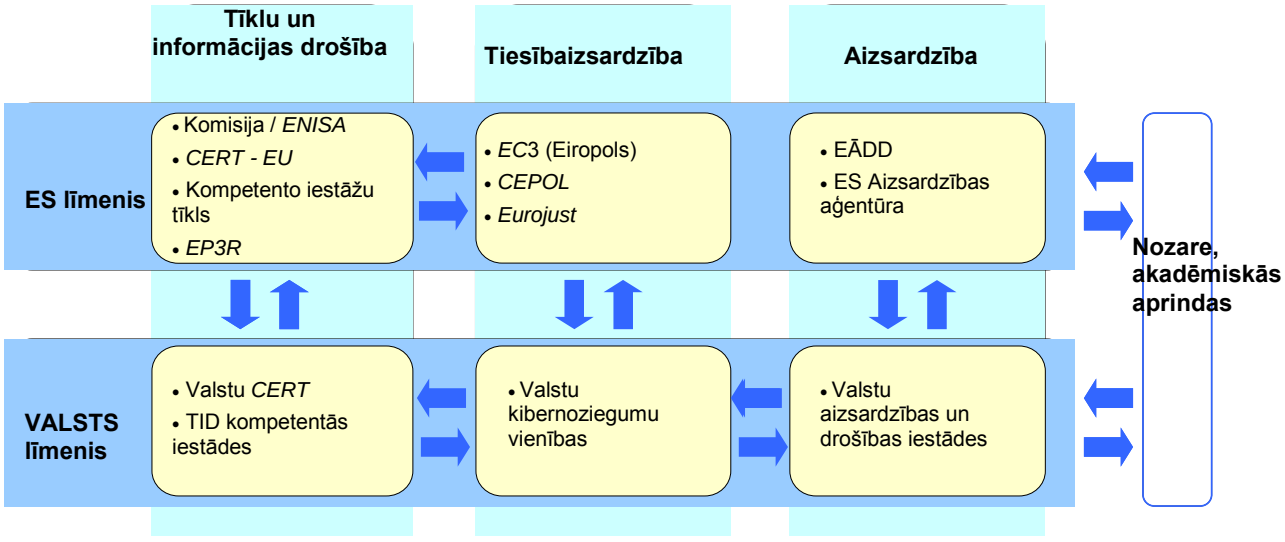
pārvaldīt spēju veidošanas iniciatīvas;

- izmantot dažādus ES atbalsta instrumentus spēju veidošanai kiberdrošības jomā, tostarp piedaloties tiesībaizsardzības darbinieku, tiesu un tehnisko darbinieku apmācībā ar mērķi vērsties pret kiberdraudiem, kā arī atbalstot trešās valstīs atbilstošas valsts politikas un stratēģiju izstrādi un iestāžu izveidi;
- palielināt politikas koordināciju un informācijas apmaiņu, izmantojot starptautiskos tīklus informācijas kritiskās infrastruktūras aizsardzībai, piemēram, Meridiāna tīklu, sadarbību starp TID kompetentajām iestādēm un citus.

3. DALĪBNIEKU FUNKCIJAS UN PIENĀKUMI

Savstarpēji saistītā ekonomikā un sabiedrībā kiberincidenti nepazīst robežu. Visiem dalībniekiem, sākot ar TID kompetentajām iestādēm, *CERT* un tiesībaizsardzības iestādēm un beidzot ar nozari, ir jāuzņemas atbildība valsts un ES līmenī un jāsadarbojas, lai nostiprinātu kiberdrošību. Tā kā var tikt iesaistīti atšķirīgi tiesiskie regulējumi un dažādas jurisdikcijas, ES galvenais uzdevums ir noskaidrot daudzo iesaistīto dalībnieku funkcijas un pienākumus.

Ņemot vērā jomas sarežģītību un iesaistīto dalībnieku plašo diapazonu, centralizēta pārraudzība Eiropas mērogā nav piemērots risinājums. Valstu valdības atrodas visizdevīgākajā situācijā, lai organizētu pasākumus ar mērķi nepieļaut kiberincidentus un uzbrukumus un vērsties pret tiem un valsts noteiktajās politikas jomās un tiesiskā regulējuma ietvaros nodibinātu sakarus un izveidotu tīklus ar privāto sektoru un sabiedrību. Vienlaikus tā iemesla dēļ, ka riskiem varētu būt vai faktiski ir pārrobežu raksturs, efektīvai darbībai valsts līmenī bieži būtu nepieciešama rīcība ES līmenī. Lai garantētu visaptverošu kiberdrošību, darbībām vajadzētu aptvert trīs galvenos pīlārus: tīklu un informācijas drošību, tiesībaizsardzību un aizsardzību, un katram no tiem ir arī atšķirīgs tiesiskais regulējums.



3.1. Koordinācija starp TID kompetentajām iestādēm/*CERT*, tiesībaizsardzības un aizsardzības iestādēm

Valsts līmenis

Dalībvalstīs jau šobrīd vai šīs stratēģijas īstenošanas rezultātā vajadzētu būt struktūrām, kas nodrošina kibernoturību, vēršas pret kibernoziedzību un garantē aizsardzību, un tām vajadzētu būt nepieciešamajām spējām rīkoties kiberincidentu gadījumā. Tomēr ņemot vērā to, ka dažām struktūrām var būt operatīvi pienākumi vairākās kiberdrošības jomās un ka ir būtiski iesaistīt privāto sektoru, ministrijās vajadzētu uzlabot koordināciju valsts līmenī. Dalībvalstīm savās kiberdrošības stratēģijās vajadzētu noteikt dažādo valsts struktūru lomu un pienākumus.

Vajadzētu veicināt informācijas apmaiņu starp valsts struktūrām un privāto sektoru, lai dotu iespēju dalībvalstīm un privātajam sektoram saglabāt vispārēju pārskatu par dažādajiem draudiem un labāk izprast jaunās attīstības tendences un metodes, ko izmanto, gan veicot kiberuzbrukumus, gan ātrākai reaģēšanai uz tiem. Izstrādātiem TID sadarbības valsts plāniem, kas jāizmanto kiberincidentu gadījumā, vajadzētu dot iespēju dalībvalstīm skaidri noteikt dalībnieku funkcijas un pienākumus un uzlabot reaģēšanas pasākumus.

ES līmenis

Tāpat kā valsts līmenī, arī ES līmenī par kiberdrošību ir atbildīgi vairāki dalībnieki. Konkrēti trīs aģentūras – *ENISA*, Eiropols/*EC3* un EAA – darbojas attiecīgi TID, tiesībaizsardzības un aizsardzības jomā. Šīm aģentūrām ir valdes, kurās ir pārstāvētas dalībvalstis, un tās veido platformu darbību koordinēšanai ES līmenī.

Starp *ENISA*, Eiropolu/*EC3* un EAA koordinācija un sadarbība tiek veicināta vairākās jomās, kurās tās darbojas kopīgi, jo īpaši analizējot attīstības tendences, veicot riska izvērtējumu, īstenojot mācības un apmainoties ar paraugpraksi. Šīm aģentūrām vajadzētu sadarboties, vienlaikus saglabājot savu specializāciju. Šīm aģentūrām kopā ar *CERT*-ES, Komisiju un dalībvalstīm vajadzētu atbalstīt uzticamas tehnisko un politikas ekspertu kopienas izveidi šajā jomā.

Koordinēšanas un sadarbības neformālos kanālus papildinās strukturētākas saiknes. ES militāro štābu un EAA kiberaizsardzības darba grupu var izmantot aizsardzības koordinācijas pasākumiem. Eiropola/*EC3* programmu vadības valdē būs pārstāvētas *Eurojust*, *CEPOL*, dalībvalstis[31], *ENISA* un Komisija, un tā dos iespēju apmainīties ar atšķirīgo zinātību un nodrošināt to, ka *EC3* darbības tiek veiktas, sadarbojoties visiem dalībniekiem un atzīstot viņu papildu zināšanas un pilnvaras. Jaunajām pilnvarām, kas piešķirtas *ENISA,* vajadzētu nodrošināt plašākas saiknes ar Eiropolu un nozares pārstāvjiem. Īpaši būtiski ir tas, ka Komisijas leģislatīvais priekšlikums par TID izveidotu satvaru sadarbībai, izmantojot TID kompetento iestāžu tīklu, un veicinātu informācijas apmaiņu starp TID un tiesībaizsardzības iestādēm.

Starptautiskais līmenis

Komisija un Augstā pārstāve kopā ar dalībvalstīm nodrošina saskaņotu starptautisku darbību kiberdrošības jomā. Šādi rīkojoties, Komisija un Augstā pārstāve aizstāvēs ES pamatvērtības un veicinās mierīgu, atvērtu un pārredzamu kibertehnoloģiju izmantošanu. Komisija, Augstā

[31] Izmantojot pārstāvību ES darba grupā kibernoziedzības jomā, ko veido dalībvalstu ES kibernoziegumu vienību vadītāji.

pārstāve un dalībvalstis iesaistīsies politikas dialogā ar starptautiskajiem partneriem un starptautiskajām organizācijām, piemēram, Eiropas Padomi, ESAO, EDSO, NATO un ANO.

3.2. ES atbalsts liela kiberincidenta vai uzbrukuma gadījumā

Lieliem kiberincidentiem vai uzbrukumiem varētu būt ietekme uz ES dalībvalstu valdībām, uzņēmumiem un iedzīvotājiem. Šīs stratēģijas (un jo īpaši TID direktīvas) īstenošanas rezultātā būtu jāgūst labāki rezultāti, novēršot un atklājot kiberincidentus un vēršoties pret tiem, un dalībvalstīm un Komisijai vajadzētu detalizētāk informēt vienai otru par lielākajiem kiberincidentiem vai uzbrukumiem. Tomēr reaģēšanas mehānismi atšķirsies atkarībā no incidenta veida, lieluma un pārrobežu ietekmes.

Ja incidents būtiski ietekmē darbības nepārtrauktību, TID direktīva ierosina, ka valstu vai Savienības TID sadarbības plānus piemēro atkarībā no incidenta pārrobežu ietekmes. Lai šajā sakarā apmainītos ar informāciju un sniegtu atbalstu, tiktu izmantots TID kompetento iestāžu tīkls. Tas ļautu saglabāt un/vai atjaunot skartos tīklus un pakalpojumus.

Ja šķiet, ka incidents ir saistīts ar noziegumu, būtu jāinformē Eiropols/*EC*3, lai tie kopā ar skarto valstu tiesībaizsardzības iestādēm varētu sākt izmeklēšanu, saglabāt pierādījumus, noteikt pārkāpējus un visbeidzot nodrošināt viņu saukšanu pie atbildības.

Ja šķiet, ka incidents ir saistīts ar kiberspiegošanu vai valsts atbalstītu uzbrukumu, vai arī tas skar valsts drošības aspektus, valsts drošības un aizsardzības iestādes brīdinās attiecīgās citas valsts iestādes, lai tās būtu informētas par uzbrukumu un varētu aizstāvēties. Tādā gadījumā tiks iedarbināti agrīnas brīdināšanas mehānismi un, ja nepieciešams, krīzes pārvaldības vai citas procedūras. Īpaši smags kiberincidents vai uzbrukums varētu būt par pamatu tam, ka dalībvalsts piemēro ES solidaritātes klauzulu (Līguma par Eiropas Savienības darbību 222. pants).

Ja šķiet, ka incidentā ir notikuši personas datu aizsardzības pārkāpumi, būtu jāiesaista valsts datu aizsardzības iestādes vai regulatīvās iestādes saskaņā ar Direktīvu 2002/58/EK.

Visbeidzot, vēršoties pret kiberincidentiem un uzbrukumiem, varēs izmantot kontaktu tīklus un starptautisko partneru atbalstu. Tas var attiekties uz kaitējuma tehnisku mazināšanu, kriminālizmeklēšanu vai reaģēšanas mehānismu krīžu pārvaldībai iedarbināšanu.

4. SECINĀJUMI UN TURPMĀKĀ RĪCĪBA

Šajā ierosinātajā Eiropas Savienības kiberdrošības stratēģijā, ko iesniegusi Eiropas Komisija un Savienības Augstā pārstāve ārlietās un drošības politikas jautājumos, ir izklāstīts ES redzējums un nepieciešamās darbības, pamatojoties uz iedzīvotāju tiesību efektīvu aizsardzību un piemērošanu, kā padarīt ES tiešsaistes vidi par drošāko pasaulē[32].

[32] Stratēģijas finansējums paredzēts plānotajā apjomā katrai attiecīgajai politikas jomai (Eiropas infrastruktūras savienošanas instruments (*CEF*), "Apvārsnis 2020", Iekšējās drošības fonds, KĀDP un Ārējā sadarbība, jo īpaši Stabilitātes instruments), kā tas noteikts Komisijas priekšlikumā par daudzgadu finanšu shēmu 2014.–2020. gadam (finansējums atkarīgs no budžeta lēmējinstitūcijas apstiprinājuma un galīgajām summām pieņemtajā DFS 2014.–2020. gadam). Lai nodrošinātu vispārēju saderību starp decentralizetajām aģentūrām pieejamo amata vietu skaitu un pakārtoto maksimālo robežu decentralizētajām aģentūrām katrai izdevumu kategorijai jaunajā DFS, aģentūras (*CEPOL*, EAA, *ENISA*, *Eurojust* un Eiropols/*EC*3), kurām ar šo paziņojumu tiek uzticēti jauni uzdevumi, tiks mudinātas tos pildīt tādā mērā, kādā būs pieejamas aģentūras jaudas jaunu līdzekļu apguvē un būs pārbaudītas visas iespējas līdzekļu pārdalei.

Šis redzējums ir īstenojams tikai godīgā partnerībā starp daudziem dalībniekiem, tiem uzņemoties atbildību un iesaistoties jauno uzdevumu izpildē.

Tādēļ Komisija un Augstā pārstāve aicina Padomi un Eiropas Parlamentu apstiprināt stratēģiju un palīdzēt īstenot izklāstītās darbības. Tāpat nepieciešams spēcīgs atbalsts un apņemšanās no privātā sektora un pilsoniskās sabiedrības, kas ir galvenie dalībnieki, nostiprinot iedzīvotāju tiesību drošības un aizsardzības līmeni.

Ir pienācis laiks rīkoties. Komisija un Augstā pārstāve ir apņēmības pilnas strādāt kopā ar visiem dalībniekiem, lai sasniegtu Eiropai nepieciešamo drošības līmeni. Lai nodrošinātu to, ka stratēģija tiek īstenota nekavējoties un izvērtējot iespējamās attīstības tendences, tās pēc 12 mēnešiem sapulcinās visus iesaistītos dalībniekus augsta līmeņa konferencē un izvērtēs gūtos rezultātus.